DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIA SUPPLEMENT I
AFI 33-113
10 JUNE 1996

Communications

TELECOMMUNICATIONS CENTERS AND DATA PROCESSING CENTER MANAGEMENT

NOTE: AFI 33-113, 30 June 1994, is supplemented as follows:

This supplement implements Air Force Policy Directive 33-1. Use this instruction with AFPD 33-1. See AFI 33-113 attachment 1, for a glossary of references, abbreviations, and acronyms used in this supplement. Sections A and B contain a list of references, abbreviations and acronyms used in the critical intelligence communications (CRITICONM community. This instruction provides procedures and responsibilities for implementing Air Intelligence Agency (AIA) Communications Operations. It does not apply to AIA-gained Air National Guard or Air Force Reserve units.

SUMMARY OF REVISIONS

(AIA) This is the initial publication of AFI 33-113, AIA Supplement 1. It replaces AFICR 700-7, 6 November 1992, and AFICR 700-6, 18 September 1992. This publication includes the AIA requirements for operating and managing a CRITICOMM support facility (CSF), remote CSF (RCSF), customer operated remote (COR), data processing center (DPC) and telecommunications center (TCC).

Section A-The Base Command, Control, Communications, and Computer (C4) System Officer (CSO)

1.3. (Added) The Unit CSO and the Unit Commander with a DPC:

1.3.l. (Added) Commanders at all levels control electrical messages. This includes restricting authority to release IMMEDIATE and higher-precedence messages to persons who have essential operational functions during crises. At HQ AIA, this authority is delegated to the Air Force Information Warfare Center (AFIWC) Information Operations Center staff duty officer, directorates, and individuals designated by them. Commanders of AFIWC, Joint Command and Control Warfare Center (JC2WC), centers, wing and group commanders, and their designated individuals, are specifically authorized to release IMMEDIATE and higher-precedence messages. Readiness center chiefs are authorized to release IMMEDIATE and higher-precedence messages when these areas have been activated by proper authority.

1.4. (Added) Unit CSO:

1.4.1. (Added) The CSO is directly responsible to the AIA unit commander for management of C4I operations, security, programs, and resources. For units that do not have an Director of Communications and Information (SC), the commander may appoint an office of primary responsibility (OPR) to carry out the C4I management duties and responsibilities described in this instruction.

- Ensures readiness of the information processing equipment and personnel to support the needs of the users.
- Monitors and evaluates operations and implements procedures to improve operations. If a service is no longer required, the CSO initiates a computer systems requirements document (CSRD) to terminate the service.
- Ensures procedures are established to cover control, handling, security, upkeep, care, reuse, and storage of message mediums.
- Ensures output products are picked up at the CSF, RCSF, TCC, and DPC only by the user, user's authorized representative, or forwarded through the base information transfer system (BITS) for collateral message traffic.
- Ensures excess equipment is identified and disposition action initiated.
- Develops operating instructions as needed and ensures they are reviewed annually for currency and accuracy. Documents the review.

Supersedes AFICR 700-6, 18 Sep 1992, and 700-7, 6 Nov 1992. Certified by: AIA/SC (Col James M. Enger)
OPR: HQ AIA/ SCXI (Mr. Edward Jolly) Pages: 25/Distribution: F;X: AUL/LSE (1),HQ AIA/ISG /SDNV (2)

- Ensures a training program is developed and maintained according to AFI 36-2202, and AFPD 36-22. The CSO should be familiar with the procedures in AFI 36-2202.
- Ensures contingency plans are reviewed at least once a year.
- Ensures adequate destruction facilities are available to meet the needs of the CSF, RCSF, TCC, and DPC.
- Ensures a customer education and support program is established to emphasize the efficient and effective use of the communications-computer systems under the CSO purview. As a minimum, this program contains the following:
- How to prepare outgoing message traffic including, floppy diskette handling procedures.
- A policy statement indicating that customers must bring message traffic to the CSF, TCC or RCSF as soon as possible after the date-time-group has been assigned.
- Use of special handling designators.
- Use of address indicating group (AIG).
- Use of defense special security communications system address group (DAG).
- Customer responsibilities such as prompt delivery of products to the CSF, RCSF, and DPC for transmission or processing and proper marking and receipt for classified products.
- Use of service action request and tracer action.
- Customer responsibilities for operating and maintaining remote terminals including outage reporting procedures.
- Emphasis on using the postal system or official organization electronic e-mail vice electrical transmission on routine precedence correspondence.
- Timely pickup of products, and notification to the DPC of processing schedule changes or delays as soon as possible.
- Contingency and alternate site agreements, plans, requirements and procedures. Ensure users also understand the processing limitations expected when such plans are invoked.
- MINIMIZE procedures and responsibilities.
- Remote terminal security.
- Focal point to resolve communications-computer system complaints and problems.
- Establishing a one-stop-shop help desk.
- Training available including assistance in understanding the technical processing aspect of their respective systems.
- Minimizing product copy requirements.
- Bulk delivery of products.

Section B-Facility Management

2.1. (Added) The wing or group CSO oversees the implementation of AIA policy related to the management and operations of C4I within its theater of operation. The unit CSO is the OPR for C4I operations.

2.2. (Added) CSF RCSF and DPC Managers.

- Unit CSO ensures that the layout of the communications-computer section promotes an efficient operation.
- Ensures primary and emergency power is adequate for their communications-computer operations and advises appropriate personnel of power problems.

- Ensures a cost-effective approach in managing resources.
- Ensures that realignment or reconfiguration of operators leads to manpower reductions, or more effective utilization of assigned resources.
- Ensures adequate scheduling of personnel during peak periods.
- Ensures that fully qualified personnel are assigned message preparation duties during heavy traffic periods.
- Ensures that the number of personnel assigned to overhead administrative management positions are kept to a minimum, to allow proper staffing of operational areas.

2.3. (Added) Facility Management Policy. Facilities housing communications-computer systems must meet the minimum requirements of this section.

2.3.1. Establish local procedures for security according to the requirements in AFI 31-209. CSF's, TCCs and DPCs containing COMSEC equipment and material must protect it as required.

2.3.2. Authorized visitors to the CSF, TCC, DPC, or computer room are allowed as long as they have the proper security clearances and the visitors do not disrupt operations. All persons entering the facility that do not require daily access, must sign in on the visitors' register and be escorted by a cleared individual at all times. During staff assistance visits (SAVS) and Inspector General visits (IG), an authorization letter of visiting personnel is posted along with the normal access list to accommodate visitors. CSF, RCSF, or DPC personnel must constantly be alert for possible sabotage or inadvertent disruptions. Persons are not allowed to enter the CSF, RCSF, TCC, or DPC if they are carrying any magnetic recording or transmitting device that may interfere with or damage equipment or supplies. All objects (such as brief cases, closed cartons, handbags) will be examined for content. Anyone refusing will be denied access.

- Fire or Safety Practices in the CSF, RCSF, TCCs or DPC. Establish safety and fire practices according to the standards in Air Force Occupational Safety and Health (AFOSH) instructions AFI 91-301 and AFI 32-2001.
- All CSF, RCSF, TCC or DPC personnel are trained annually on fire suppression systems and fire reporting procedures. Training includes, as a minimum, fire evacuation routes, proper use of fire fighting equipment, and fire fighting techniques. Fire drills are conducted at least semiannually. Both training and drills are documented as recurring training. Manual suppression of the halon system is included in the training program to preclude unnecessary recharging of the system because of false alarms. The rules in the AFOSH services standards apply to all communications-computer systems operations. Where the possibility of electrical shock exists, safety equipment is provided. Equipment operators are trained to use the electrical safety equipment and trained in an approved method of cardiopulmonary resuscitation (CPR) annually.
- Emergency Lighting. Emergency battery operated lighting is provided to ensure the safe shutdown of equipment and exit of personnel in case of total power failure.
- Environmental Control and Temperature and Humidity. Maintain environmental conditions according to equipment specifications and establish emergency procedures for environmental equipment failures. Retain the recording charts according to AFI 37-133, Volume 1. CSFS, TCCs or DPCs that have an energy management control system do not require recording devices.

2.4. (Added) Facility Equipment Room Cleanliness:

- CSF, RCSF, or DPC equipment rooms must be kept free of dust. Air conditioner filters must be checked monthly and changed as required.
- Tile covered floors will be kept clean. Steel wool buffing pads will not be used.
- Installed raised floors will not be wet mopped. Inspect subfloor under the raised floor at least once every 60 days and clean as necessary.
- Carpeting, when used in equipment rooms, must comply with vendor contract specifications.

- Eating and drinking is not permitted while directly involved in operating equipment, and is only allowed within a designated area of the larger room, if there is not an available area off the CSF, RCSF, TCC, or DPC floor. This area must be more than five feet from any ADP equipment, cryptographic equipment, or tape libraries. A partition should be used to set off the break area from the rest of the room. It is critically important that food and drink are kept away from equipment and diligent efforts are made to ensure that beverages are not spilled on raised floors.

2.5. (Added) Storage Areas. Adequate storage space is provided for communications-computer systems equipment supplies, and input and output material. Operators should condition paper stock by subjecting them to environmental conditions similar to those of the computer room if possible.

2.6. (Added) Supply. An adequate supply of items of paper, diskettes. magnetic tape, and disk packs requires advance planning, budgeting and continuing review to ensure they are available at the appropriate time and in the required quantity and quality.

2.6.1. **Stock Levels.** The CSF, RCSF, or DPC manager coordinates with the publications distribution office and the unit supply liaison to establish and maintain stock levels. Records of supply use is maintained for management purposes.

2.6.2. **Defective Supplies.** Forms, ribbons, paper, etcetera, must meet required specifications. Machine failures, work stoppage, and processing failures due to inferior supplies is documented. Procedures for reporting blank form deficiencies are in AFI 37-160, Volume 8. Report other material deficiencies to base supply or the base contracting office, whichever is appropriate.

2.6.3. **Disposal.** Dispose of unused or excess paper stocks and special forms that have accumulated through normal processing according to DoD Manual 4160.21. Destroy papers on personal data or sensitive information recorded according to the privacy act requirements listed in AFI 37-132 and AFI 33-202. Destroy classified waste according to DoD 5200.1-R, AFI 31-101 Vol 1 and USAFINTEL 201-1. All burnable waste must be destroyed as classified, if the CSF, RCSF, or DPC uses cryptographic equipment. Place specifically marked containers in break areas for unclassified nonburnable waste (such as cans, bottles, ribbon spools, etcetera).

Section C--Operations Management

3. (Added) Operations Management Policy. This section provides policies for managing the operation of communications-computer systems and facilities.

3.1. (Added) Basic Responsibilities. Managers must be responsive to mission and customer needs and use management principles which leads to effective mission support at the lowest cost.

3.2. (Added) CSFs and RCSFs use standards or other measurements as developed by Allied Communications Publications (ACP), Defense Information Systems Agency (DISA) circulars, Joint Army, Navy, Air Force Publications (JANAP), Field Operating Agency (FOA) and other directives applicable to evaluate performance.

3.3. (Added) Inventory, accountability, and performance records are kept to allocate work, develop standards or norms, and plan future work. In addition, they are used to compute rental or maintenance charges, discounts, credits, liquidated damages, and to verify that communications-computer systems equipment is used for approved applications and products. All communications-computer systems records are maintained as required in AFI 37-133 Vol 1.

3.4. (Added) Communications personnel may not alter the contents of information systems products except with permission of the originator or releaser. Document authorized changes by entering the originator or releasers name, date, and time in the master station log.

3.5. (Added) Communications personnel may not divulge, release, or publish the contents of information systems products (including voice) to any person other than the addressee, addressee's representative, or person authorized by local or command directives. Refer persons who request access to information systems products to the originator or addressee of the material.

3.6. (Added) Operations During Severe Weather Conditions. When severe weather conditions exist (electrical or thunderstorms within 10 statue miles of an installation, ice storms, high wind conditions, etcetera), the CSF, TCC, or DPC will normally power down their equipment, unless the customer or user's mission dictates otherwise as in computer facilities operated in the client-server environment. The CSO ensures local procedures are developed and implements those procedures based on an evaluation of weather reports, contractual liabilities, and user mission requirements to determine if the equipment should remain powered up. Any CSF, RCSF, TCC, or DPC whose users must continue processing during severe weather conditions on a recurring basis will install an alternate power source, such as a motor generator, to ensure processing continues with no interruption to the customer (see AFI 25-501 for host tenant support agreements).

3.7. (Added) Contingency and Alternate Site Agreements, Plans, Requirements, and Procedures.

- Every systems manager is responsible for developing and coordinating detailed plans to support operations under emergency conditions. The CSO must develop, test, and maintain contingency plans required to support unit and base plans.
- Managers must prioritize critical systems according to mission requirements in the contingency plan. Consider factors such as:
- The importance of the mission that the system supports.
- The adverse impact on the operation (such as lowered productivity, inability to respond to operational needs, and so forth).
- The additional cost of recovering from a system outage.
- Contingency and recovery plans:
- Describe the actions necessary to ensure continuity of operations in the event of a disaster or to restore operation in the event of a system failure.
- Vary in length depending on the critically of the system.
- Must include steps for:
- Emergency preparation.
- Interim processing requirements.
- Software and data backup strategy.
- Equipment maintenance concept.
- To ensure minimum disruption of operations and support, backup data files must be positioned in off-site storage locations, if possible and available. In addition, one or more alternate processing sites may be identified, if the security classification, systems, and material permits. Alternate site agreements are reviewed on an annual basis. Each CSF and RCSF establishes a contingency and alternate site agreement for processing incoming and outgoing messages in the event communications become totally disabled. This agreement should be established for both Defense Special Security Communications System (DSSCS) and General Service (GENSER) traffic handling. CSFs, DPCs, or CORs unable to establish such an agreement advises HQ AIA/SCXI on the reasons the agreement cannot be established. For those stations that are directly connected to AUTODIN, submit your alternate routing requests according to DISA OPLAN 1-84.

3.8. (Added) Operating Procedures. Develop operating instructions as needed and ensure they are reviewed annually for currency and accuracy.

3.9. (Added) In addition to those suggested items for operating procedures listed in AFI 33-113, attachment 3. The following areas are suggested:

a. References

b. Field Operating Agency Publications.

AIADIR 37-130, Headquarters, Air Intelligence Agency Staff Directory.

AIADIR 37-135, (C) Air Intelligence Agency Subordinate and Supported Activity Address Directory (U).

c. NSA/CSS Publications. COIs and DOIs are ordered directly from NSACSS/Q312. Units ordering publications must be listed in USSID 505 Annex A or DIA Compartmented Address Book.

COI-101, (S) Critical Intelligence Communications Systems (CRITICOMM Operating Instructions General (U).

COI-104, (C) CRITICOMM Operating Instructions Facilities Control Procedures (U).

DOI-102, (S-HVCCO) DSSCS Operating Instructions (U) Routing Indicators.

DOI-101, (S-HVCCO) Defense Special Security Communications System (DSSCS) Address Groups.(U)

DOI-103, (C) Defense Special Security Communications System (DSSCS) Operating Instructions (U) System/Data Procedures.

USSID-505 Annex A, (S-HVCCO) SIGINT Organizations (FOUO).

USSID-507, (C-HVCCO) SIGINT MINIMIZE Procedures (FOUO).

USSID-508, (C-HVCCO) Use of Operations Communications (OPSCOMM (FOUO).

USSID-519, (TS-ITVCCO) Delivery Distribution Indicator (DDI) (FOUO).

USSID-536 (C) Telecommunications Field Engineering Support Program (FOUO).

USAFINTEL 201-1, (S-HVCCO) Security Use, and Dissemination of Sensitive Compartmented Information (SCI) (U).

3.10. (Added) Address Indicator Group (AIG) Management. The Policy Branch (HQ AIA/SCXI) is responsible for AIG assignments within the agency. Forward your AIG assignment request to that office. Originators and recipients of AIGs provide their servicing CSF or RCSF copies of newly established, recapitulations, modification, or cancellations of AIG messages on which they are an addressee. The CSF or RCSF cannot ensure delivery unless they are provided current information.

a. Responsible Authority. The responsible authority for an AIG is the activity charged with overseeing an AIG's use and administration. The responsible authority:

(1) Ensures that each assigned AIG is required and that its address composition is kept current.

(2) Ensures that only authorized message originators use the AIGs as directed by HQ AIA/SCXI.

(3) Sends AIG modifications, cancellations, and recapitulations to the CSF or RCSF, ATTN: AIG Manager, addressees, and user at least 5 days before the effective date unless emergency dictates otherwise. Ensure NAVCSRF HONOLULU HI//N33// is an information addressee.

(a) Modification of an AIG consists of addressee additions, deletions, and changes.

(b) Cancellation of an AIG consists of identifying AIGs that are no longer needed and publishing a notice terminating their use.

(c) Recapitulation of an AIG consists of publishing an accurately revised total address composition, cognizant authority, authorized users, purpose and point of contact. Do this when numerous modifications have been made, but at least once a year during the 12th month following initial establishment or last recapitulation.

(d) Send promulgation's, modifications, cancellations, or recapitulations of AIGs which include naval units at sea or mobile units as addressees to Naval Telecommunications System Integration Center (NAVTELSYSSIC), NAVCOMU, Washington DC 20301; Naval Communications Area Master Station Atlantic (NAVCAMSLANT), Norfolk VA 23511; and Naval Communications Area Master Station East PAC (NAVCAMS EASTPAC), Honolulu HI 96318, for information.

b. AIG Address Composition. Use addressees for Air Force activities listed in AFDIR 37-135 in the address composition of the AIGS. For other DoD, Army (USA), and Navy (USN) addressees, use the PLA as indicated in Department of the Army (DA) Pamphlet 25-11, USN PLAD 1, or USMCEB Publication Number 6 (all are part of AFD 37-135). Do not:

(1) Create AIGs with less than 16 addressees.

(2) Use the locations of emergency relocation sites (ERS), alternate headquarters (ALT HQ (ACP 117 US SUP-4), naval units afloat, mobile units, or task force organization addressees.

(3) Use collective address designators, such as general message titles.

(4) Include commands or activities served by commercial means. (Contact your servicing CSF or RCSF for assistance in this area).

(5) Include addresses of other nations, International Pact Organization (IPO), non-DoD or DoD addresses served by non-DoD telecommunications facilities unless you have prior coordination and a statement to that effect in the request for assignment of an AIG.

c. AIG User Responsibilities. Only the responsible authority and those activities designated by the responsible authority may use an AIG. The following applies:

(1) To prevent sending an AIG message to an incorrect AIG number, spell out AIGs and only address them as "ACTION" addressees. If an AIG is sent for "INFORMATION," type it as an action addressee (example: TO AIG EIGHT FIVE FIVE THREE), and state in the first line of the message text "AIG EIGHT FIVE FIVE THREE TAKE FOR INFORMATION ONLY".

NOTE: If a TCC or DPC communications facility require numeric numbers (that is AIG 9550) on outgoing messages, management will advise their customers of this requirement in their Customer Education Brochure or Program.

(2) When using two or more AIGs and an addressee is listed in more than one AIG, CSFs and RCSFs must prevent duplicate delivery of terminated message traffic, (NEWSDEALER systems automatically prevents duplication of addressees on AIGS).

(3) Add-on addressees may not know the address composition of the addressed AIGS. If the originator thinks this information is important to the add-on addressees, the originator will provide them the address list upon request.

(4) Addressees may be exempted from an AIG by entering the addressee as the last information address with "XMT" preceding the address element. Example: XMT DET 1 488 IS RAF DIGBY UK.

d. AIG Addressee Responsibilities. Addressees must tell their servicing CSF or RCSF when they are included in an AIG and if they are authorized to use the AIG. They must also furnish a copy of any promulgation's, recapitulations, modifications, or cancellations of the AIG.

(1) Do not readdress AIG messages, except in operational emergencies, unless the readdressing action is to addressees that were not included in the original transmission. If the operational urgency of the subject does not allow time for an AIG address composition review, the message may be readdressed with add-on addressees.

(2) If addressees determine that they no longer need to be included in an AIG or if their titles or addresses change, they will tell the responsible authority.

(3) Upon relocation to or activation of an ALT HQ. or ERS. the agency notifies the responsible authority and other authorized AIG users. Prompt notification to CSFs and RCSFs will ease message processing.

e. Security Classification of AIGS. Before classifying the address composition of an AIG, the responsible authority must carefully consider:

(1) If an ERS or ALT HQ is addressed without giving its location. the address composition may be unclassified.

(2) If the address composition has classified or sensitive order-of-battle information., it should be classified.

(3) If correspondence dealing with classified AIGs contains any information which can be associated with the AIG address composition, classify it at least Confidential. However, modifications to a classified AIG need not be classified if the modification does not give any sensitive information which formed the basis for the original security classification.

f. Numbering AIG Modifications:

(1) Give each AIG modification a sequential number. Number modifications continuously until the AIG is recapitulated.

(2) Show the identification of the modification in the subject line of the letter or message as follows: the abbreviation AIG, the AIG number, a slant (/) sign, and a modification number. For example, SUBJ: AIG 8553/4 MODIFICATION.

(3) Each recapitulation is modification number one, thereby starting a new series of modification numbers. When a recapitulation includes modifications, take care to include addressees that are being deleted or added to the AIG in the address of the message. The text of the recapitulation identifies those activities being added or deleted, or amended.

g. Request for AIG Information. Forward information requests concerning the identification of the responsible authority on those AIGs for which HQ AIA/SCXI is the issuing agency to your local CSF or RCSF. If the responsible authority of the AIG is unknown, forward your request to HQ AIA/SCXI. For those AIGs not issued by HQ AIA/SCM, forward your request with as much identifying information to your local CSF or RCSF. If they cannot assist you, they will obtain assistance from HQ AIA/SCXI.

h. CSF and RCSF Responsibilities for AIGS. Maintain a separate folder for each incoming and outgoing AIG message addressed to or from the unit. These folders are used to provide customer support pertaining to AIG messages. The folders contain the following messages:

(1) AIG promulgation's and, or establishment (messages and letters).

(2) AIG recapitulations.

(3) AIG modification correspondence (messages and letters). When the AIG is canceled by the responsible authority, the folder is destroyed according to AFR 4-20.

3.11. (AIA Added). Submit request for GENSER routing indicators using the format prescribed in ACP-117 CAN-US SUPP-1, para 15f. Address your request action to HQ AIA DIR OF COMMAND INFO KELLY AFB TX//SCXI//, info your intermediate headquarters, and AFCPA WASHINGTON DC//SMCTR// and any other addressees you deem appropriate.

3.12. (Added) Submit request for DSSCS routing indicator using the format prescribed in DOI-102, Section 4. Assignments, Deletion and Change. Before a DSSCS routing indictor can be assigned, the organization that is being requested for must be listed in USSID-505 Annex A and or the DIA Compartmented Address Book (DIACAB). If they are not listed in one of these publications, action is taken by the requesting organization to have the unit included. Address your request action to HQ AIA//SCXI//, info your intermediate headquarters, NSACSS//Q312// and any other addressees you deem appropriate.

3.13. (Added) Submit request for changes to AFDIR 37-135, action to 67SUPTS//IM//, info (HQ AIA/SCXI). To ensure the change is made in AIADIR 37-130.

3.14. (Added) MINIMIZE. MINIMIZE is a condition that a commander or other authority impose on users of telecommunication systems in an emergency or exercise. The aim is to limit the volume of routine traffic in the communications system and ensure the flow of essential traffic. Essential traffic is that which deals directly with the success of the mission or safety of life. For DSSCS minimize information, consult DOI-103, USSID 507 and USSID 508.

a. Basis for Imposition. The need for MINIMIZE is a decision the commander must make based, in part, on the following:

(1) Capability to act on orders from higher headquarters.

(2) Impact on subordinates and on other commanders.

(3) Operational necessity, based on present indications or past experience.

(4) Excessive loading of the communications networks, particularly those switched networks of the Defense Information Systems Network (DISN), and automated digital network (AUTODIN).

b. Application. Commanders may impose MINIMIZE on all those who use United States military telecommunications, however, before this is done, the scope of its applicability must be weighed. Commanders must limit MINIMIZE to the least number of users affected by the emergency or exercise. For example, a cable break that stops communications from Guam to Okinawa need not call for MINIMIZE in the whole Pacific. As changes in the situation make it necessary, MINIMIZE may be expanded, reduced, or canceled completely.

c. Imposition Authority. Commanders may impose MINIMIZE on their command or a part of their command unless prohibited by higher headquarters. They may also ask other commanders and chiefs of government agencies to impose MINIMIZE on all users who communicate with activities in the MINIMIZE area. MINIMIZE imposition authority is as follows:

(1) Worldwide. Only the JCS has the authority to impose MINIMIZE worldwide on all users of GENSER message traffic. DIRNSA shall determine when DSSCS MINIMIZE is to be imposed on CRITICOMM facilities. See DOI-103, USSID 507, and COI-1011, chapter 6.

(2) Within AIA, the Commander of AIA may impose MINIMIZE only on voice or record communications originated within AIA.

(3) Automatic imposition. MINIMIZE is automatically imposed on those who use record and voice communications when defense readiness conditions (DEFCON) 1 and 2 are declared.

d. Planning. Planning is essential if MINIMIZE is to work. Tor prepare for MINIMIZE, TCCs, CSFs, RCSFs, RCSFS, and customer operated terminals will put instructions in local directives to explain MINIMIZE and ensure compliance.

(1) Set up strict written guides to control, monitor, and evaluate the use and responsiveness of communications facilities during MINIMIZE.

(2) Identify reports to be sent by nonelectrical means during MINIMIZE. Inform customers of the requirements of MINIMIZE.

(3) When processing outgoing messages on DD Form 173-1. Joint Message Form (Black), or floppy diskette, check the format of recurring reports to be sent electrically during MINIMIZE to see that authorized abbreviations are used.

e. Control of Communications. When MIMMIZE is imposed, control electrically recorded messages as follows:

(1) CSF and RCSF personnel:

(a) Determine if MINIMIZE is for GENSER or DSSCS. When processing outgoing messages on DD Form 173-1, or floppy diskette, put all narrative messages on hand but not yet sent, into two groups: Priority and higher-precedence messages and Routine precedence messages. Send the Priority and higher-precedence messages in the normal way. Return those that have Routine precedence to the releasing officials to see if they should be sent under MINIMIZE.

(b) Send all subsequent traffic in the normal way. Return those messages which do not have the words " MINIMIZE CONSIDERED" and the releaser's initials.

(c) The message drafter who wants to send a message stamps, types, or writes in ink "MINIMIZE CONSIDERED" on the AIA Form 156, Diskette Message Form, or the "Special Instruction' block of DD Form 173-1, and provide his or her initials.

(2) At CSFs and RCSFS: Upon receipt of a message which impose MINIMIZE, forward a copy electrically to all connected in-house and distant remote customers using general message " ALREMOTES. "

NOTE: At HQ AIA, fonvatd a copy to all customers on the Local Area Network (LAN).

(3) Cancellation or modification. The imposing or higher authority can cancel or modify MINIMIZE. The cancellation message uses the words, "CANCEL MINIMIZE," followed by the scope (area and mediums of electrical communications) or the condition to be canceled. The message canceling or modifying MINIMIZE refers to the message which imposed MINIMIZE and, if cancellation is not immediate, includes the date and time that MINIMIZE is to be canceled.

3.15. Methods and Results (M&R). M&R personnel provide quality control and statistical reporting. They provide CSF and RCSF management personnel information and recommendations on the quality of service provided to their customers.

a. Analysis Methods. M&R personnel can use various methods to check the efficiency of the CSF and RCSF operation. The two most commonly used are visual observation and statistical comparison. Visual observation consists of looking at operations in progress. Since this method gives real-time evaluation, managers must use it for analysis of rules, performance, and operator proficiency. A statistical comparison is generally an after-the-fact method for getting data and analyzing it for trends. Managers must use this type of analysis for evaluating such things as handling time, volume, and error rate.

b. Analysis Areas. There are many areas in the communications-computer system which will help performance analysis obtain information to check the effectiveness and efficiency of the CSF or RCSF. The following describes some of these areas:

(1) Customer satisfaction (effectiveness). The quality of service that the CSF or RCSF provides is measured, first, by the users of the service and, second, by the personnel operating the CSF or RCSF. Analysis personnel must perform customer visits. conduct user group meetings., and develop questionnaires to obtain user feedback. Management personnel then must use this feedback to enhance customer satisfaction and eliminate deficiencies.

(2) Internal CSF and RCSF operations (efficiency). The M&R function will take a critical look at the internal procedures. These are the more traditional areas of traffic analysis. In these areas, M&R checks various aspects to find the accuracy, speed, and reliability of message processing. In comparing the results to system standards and to the station's past records. managers can develop an accurate picture of current performances and trends.

(3) Operating Procedures. M&R will check adherence to directives (such as ACPS, JANAPs, DOIs, COIs, operating instructions, etcetera), When rules are not being followed, inform management. If there are deficiencies in the directives, make recommendations via chain of command to get them changed.

(4) Operator proficiency. Check operators' proficiency to see how well they are working and if they need training. Checks will cover all operator rules (such as CRITIC processing, message distribution, NEWSDEALER operations, etcetera).

(5) Workload. Get data on the volume of message processing in the CSF. Examine the data by analyzing the type of information, precedence, classification, DSSCS or GENSER, and peak periods. Management must use what is learned to plan work schedules, operating hours, and guides for information flow.

(6) Handling times. Check CSF and RCSF in-station handling time for processing message traffic to determine trends, problem areas, and improve processing time. Where the volume of message traffic is large, it is not practical to check every message to determine handling times. Therefore, CSFs and RCSFs will use some form of sampling which accurately shows the time used for processing. When a sample method is used, only a percentage of the total volume of message traffic is checked. The more samples selected for checking, the more accurate the standard will be. A check of approximately 5 to 10 percent of the total traffic volume over the operating period shows an accurate in-station handling time. The following criterion is used within AIA:

Defense Special Security Communications System (DSSCS):

PRECEDENCE	SPEED OF SERVICE OBJECTIVES
CRITIC	2 minutes
FLASH	6 minutes
IMMEDIATE	12 minutes
PRIORITY	33 minutes
ROUTINE	150 minutes

General Service (GENSER) Communications Systems:

CRITIC	2 minutes
FLASH	Not fixed. Handled as fast as humanly possible within objective of less than 10 minutes.
IMMEDIATE	30 minutes
PRIORITY	60 minutes
ROUTINE	180 minutes

c. Service Messages, CSFs, RCSFs, and CORs are used for exchanging information regarding misrouted, incomplete delivery instructions, or errors committed during message transmission. Service message files are used to check problem trends and help eliminate them through the use of planned training programs. Service messages directed to a remote terminal will be handled by that remote (except HQ AIA Security Hill remotes). Information and procedural assistance will be given by the host to all customers.

d. Equipment and Circuit Performance. Check the efficiency of the equipment and circuits, since they have a great effect on speed, reliability, accuracy, and security of messages processed. M&R analysis activities must bring poor trends to the attention of CSF and RCSF management personnel who must then work with the applicable agency to resolve the problems.

e. Communications Operating Performance Summary (COMOPS) and Communications Improvement Memorandum (CIM). Use the COMOPS and CIM provided under the message quality control program according to ACP 121, US Supplement I and JANAP 128. The information provided is excellent for analysis purposes, since it gives data on errors committed. M&R analysis activities try to find the cause of errors and give management personnel recommendations for eliminating them. The AIA standard regarding CIMs is .25 percent error rate.

f. For those units that receive the Communications Operations Summary (COMOPS) from the AUTODIN Switching Center, ensure they are used as a management tool and are made available for all personnel to review.

g. AUTODIN Switching Center (ASC) Staff Visits. All units ensure that deficiencies noted by an ASC staff visit are corrected. HQ AIA/SCXI and intermediate headquarters are provided a brief description of the noted deficiencies and corrective actions taken.

3.16. (Added) Retention of Messages.

a. To satisfy claims of loss or nonreceipt of messages, CSFs and RCSFs keep a temporary reference file of messages sent by the activities they service. Electronic record copies are kept for 30 days.

b. Retain:

(1) Service files 30 days.

(2) Floppy diskettes 30 days.

c. Message page copy, floppy diskettes, and records which are involved in cryptographic compromise will be retained until directed to be destroyed.

d. General messages addressed to the CSF, RCSF, TCC, DPC, or COR will remain on file, either in hard page copy or electronically, until rescinded or superseded by the responsible authority, See attachment 5 for a list of general message titles.

3.17. **(Added) Customer Education and Customer Support.**

Each CSF, RCSF, TCC, or DPC must set up and maintain a sound customer support program tailored to fit the local situation. The purpose of the program is to improve service to users by training them to use the systems effectively and efficiently. Local programs may vary in the form of presentation but each will cover all appropriate aspects of communications-computer systems. Management personnel must be intimately familiar with the mission and support required by base activities. These individuals must take the lead in establishing the forum and encouraging the free flow of information between the users and the CSF, RCSF, or DPC. The user perspective of the support being received is vital to measuring the effectiveness. Good customer relations translate to effective mission support.

a. Customer Visits. A visit by management personnel will be performed as needed to representative user locations for each automated data system (if a user is responsible for multiple systems a single visit will suffice). Management personnel will use the visits to better determine the needed user interface, pinpoint possible customer dissatisfaction, and provide visibility of the CSF, RCSF, TCC or DPCs interface and importance to mission accomplishment. Document visits made, issues discussed, and actions taken.

b. Customer Education Guide. Each CSF or RCSF will publish a Customer Education Guide to include the following as a minimum.

(1) How to handle misrouted messages.

(2) How to request service actions.

(3) Examples of PLA updates (for remote users).

(4) Requests for retransmissions.

(5) Procedures for floppy diskettes.

(6) Procedures for message transmission/formats

(7) MINIMIZE.

(8) Message Management Letters.

(9) Standardization of Plain Language Addresses (PLAS) - AFDIR 37-135,USSID 505, DIACAB, AIADIR 37-135, etcetera.

(10) Use of DAGs and AIGS.

c. Customer Questionnaires. Questionnaires are a viable method of determining customer satisfaction and for determining system weaknesses and procedural complaints before they become problems. Questionnaires should be sent to customers periodically throughout the year.

Section E--Message Handling and Administrative Procedures

4. (Added) Policy, Procedures, and Guidance. NSACSS COI-101, 103, and DOI-102 contains specific policies, procedures, and guidance for the operations and management of CSF, RCSF for CRITICOMM.

4.1. (Added) Authorized Users of the CRITICOMM System: Authorized users are those members listed in USSID 505 Annex A, DIA Compartmented Address Book, AIADIR 37-135, and those SIGINT organizations supported by AIA.

4.1.1. (Added) Handling ALA/CC or CV Messages **During Periods of Temporary Duty (TDY).** To ensure that messages addressed to, or originated by, the AIA Commander (CC) or Vice Commander (CV) during periods of TDY are handled properly, the following procedures apply:

a. The Executive Officer (AIA/CCE) provides the CC or CV's itinerary to all AIA units including Operations Support Central (AFIWC/IOC), and RCSFs to be visited.

b. Each CSF, RCSF or units visited is an addressee of all messages forwarded for the CC or CV. Only the action addressee's CSF or RCSF acknowledges receipt (ZDF-1 or ZDF-2) to AIA/CCE.

c. Each CSF, RCSF visited sets up two folders; one for incoming messages addressed to the AIA/CC or CV and one for messages originated by the AIA/CC or CV. All messages are logged on an AF Form 3531. Message Delivery Register.

d. AIA/CCE ensure that messages addressed to or from the AIA/CC or CV are sequentially numbered (1, 2, 3, etcetera) for positive control.

e. Any time a message is received and there are indications that a sequential number is missing, the CSF of the AIA unit being visited notifies AIA/CCE by IMMEDIATE precedence message or telephone call (during duty hours) and AFIWC/IOC during non-duty hours.

f. Persons preparing correspondence:

(1) Ensures that ZFF1 and ZFF4 are placed on the message following the date-time-group. Messages released on floppy disk must have a date-time-group and contains ZFFI and ZFF4. Example: 23090OZ FEB 95 ZFF1 ZFF4.

(2) For classification of CC's or CVs itineraries, see AFI 31-401/AIA Sup 1.

(3) Follow the procedures below to ensure efficient transmittal and delivery of messages addressed to or originated by the AIA/CC or CV.

(a) Any CSF or COR having problems delivering messages request guidance from AIA/CCE by immediate precedence message or telephone call during normal duty hours, and from AFIWC/IOC during other then normal duty hours.

(b) Transmit report of delivery by Priority precedence message to AIA KELLY AFB TX//CCE// (for GENSER) and AIA//CCE// (for DSSCS).

(c) Transmit requests for retransmission by priority precedence to the CSF or COR Noncommissioned Officer in Charge (NCOIC) in service message format. Dual address to originating station and info the CC's next destination if the time element dictates.

(4) The following procedures are for transmission requests:

(a) If the message is sensitive compartment information (SCI) and the noncryptologic unit is supported by an SSO Communications Center, transmit the message to the SSO with internal passing instructions. If there is no SSO-supported Communications Center, hold the message until the CC or CV arrives, and advise the message originator of your actions.

(b) If it is doubtful that the retransmission will reach the requesting stations because of the time element, dual address the retransmission to the station requesting retransmission and the commander's next destination listed on the itinerary.

5. (Added) Message Handling Procedures.

5.l. Incoming Message Processing.

5.1.1. (Added) HQ AIA supported organizations that operate communications support processors (CSP) develop procedures for message handling, both incoming and outgoing to ensure their internal, external and backside customers are provided appropriate message service.

5.1.2. (Added) Customers provide the SC personnel a message management letter (MML) which identifies personnel authorized to pick up unclassified messages, those authorized to receipt for classified messages and individuals authorized to receipt for messages requiring special handling (SPECAT, LIMDIS, etcetera). The contains the name, grade, social security number or civilian identification card number, current security access,. and specific special handling designator to which the individual has been granted access. The MML is classified as appropriate and contain the statement: "This letter contains Privacy Act Information. Release of Information herewith not to be made without written consent of individuals." For SPECAT messages, the letter designates the specific special handling or category designator for which the individual has been granted access. Do not use all inclusive phrases (such as "cleared for all SPECATS" or cleared for all SPECAT codewords"). The program and codewords are be identified in the letter and each title. and signature of the authorizing official. Authorizing officials are organization or activity commanders, and those functions within the organization as designated by the commander or the appropriate directorate chief at intermediate headquarters or agency level. The commanders' signature verifies the security access of all individuals listed on the letter. The authorization letter is updated semiannually or as changes occur.

NOTE: If an appropriate authorization list is not on file at the CSF, RCSF, or COR, the SC calls the organization or activity commander, deputy commander, acting commander, directorate,. division chief or the appropriate directorate chief at the intermediate headquarters or agency level. The commander may personally receipt for the message (after proper identification).

5.1.3. (Added) Provide the CSF or RCSF a list of representatives to be notified by telephone on receipt of priority or higher precedence messages during and after normal duty hours (24 hours). Telephone answering machines are not used to replace a person who can answer and take responsibility for the high precedence message notification. This list is reviewed and updated at least semiannually. Addressees may opt not to be notified on priority messages, but this option must be in writing and on file. This requirement may be combined with the message management letter.

5.1.4. (Added) Message addressees provides for immediate pickup of messages that are high-precedence or those that require special handling.

5.1.5. (Added) Customers must establish a central point of distribution for messages addressed below the 2-letter functional address symbol (FAS).

5.1.6. **(Added)** At CSFs which have NEWSDEALER Automated Message Handling Systems (AMIHS), unique customer profiles will be established based on the customers unique DSSCS and GENSER routing indicators and office symbols. NOTE: Profiling must be very closely monitored to ensure special handling, or other types of sensitive messages are not profiled and delivered to the wrong customer(s).

5.1.7. **(Added)** Deliver message traffic on floppy diskette to customers within and outside of a sensitive compartmented information facility (SCIF). NOTE: Within AIA ensure the TOOLBOX program "BUSTER" is run on all FLOPPY DISKETTES DELIVERED OUTSIDE OF THE SCIF. This is to ensure that messages containing SCI or HIGHER SECURITY CLASSIFICATION than the recipient is authorized to receive is not contained on the diskettes.

5.2. (Added) Outgoing Message Processing.

5.2.1. (Added) If additional copies of an outgoing message are sent by nonelectronic means, or copies for local or staff distribution, the releaser makes such delivery. The CSF will not reproduce additional copies of outgoing messages for customer-related responsibilities.

5.2.2. (Added) Electronic distribution may be effected for originated message traffic destined for any customer operated remote (COR) that is connected on line to a NEWSDEALER host. ZEN IS NOT REQUIRED.

5.2.3. (Added) Proofreading Messages. Proofread all CRITIC messages after they have been transmitted. Immediately send a voluntary correction (ZZS for DSSCS messages) on all CRITIC messages (see DOI-103 for CRITICS)

5.2.4. (Added) Interlaced Messages. CRITICOMM stations reporting interlaced messages according to DOI-103 include HQ AIA/SCXI and appropriate wing and group FAS as information addressees on the initial report and all follow-up correspondence about the interlace,

5.2.5. (Added) Keyboard Operations. Manual keyboard transmission into the line are specifically forbidden except as required for maintenance, facility control, teleconference operations, or to pass a CRITIC message.

5.2.6. (Added) Floppy Diskette. The "ABOVEBOARD" program is the software used to generate messages on floppy diskette for processing by AIA CSFs, RCSFs, or CORs.

5.2.7. **(Added)** Customers may use any word processing software and save the file as an ASCII text file.

5.2.8. **(Added)** All floppy diskettes delivered to the CSF, RCSF. or COR will be accompanied by an AIA Form 156, Diskette Message form.

5.2.9. **(Added)** Place the disk in a stand alone PC to assure that it contains only the message traffic listed on the AIA Form 156, to be sent. Also, run a VIRUS check against the disk using the TOOLBOX VIRUS check program.

5.2.10. (Added) After the messages have been transmitted, CSF or RCSF personnel verifies that no residue message traffic is on the diskette.

5.2.11. (AIA Added) The use of a local area network (LAN) to facilitate message processing (sending or receiving) is authorized.

5.2.12. (Added) Customers remoted NEWSDEALER automatically receive a FEEDBACK copy of all off messages transmitted from their remote terminal. Additionally, all ERROR messages are automatically returned to the customers terminals for correction.

5.2.13. (Added) CRITIC Message Handling. Personnel must be highly trained in handling and reporting CRITIC messages. CRITIC procedures should be memorized. Reviewing procedures for information during the processing of CRITICs is too late.

a. When transmitting a CRITIC and an acknowledgment is not received within 2 minutes, operators will retransmit the CRITIC via their alternate means, until an acknowledgment is received.

b. When the 2 minute threshold, 120 seconds is exceeded, explain the reason for not meeting the standard handling time in the CRITIC Handling Report (NSA RCS-972) paragraph four.

c. Supervisors assign persons on each shift specific tasks in processing CRITIC messages; preempting circuits, calling up prepared CRITIC headers, preparing text, and transmitting messages.

d. Ensures that each CRITICOMM facility that supports an operational mission has a CRITIC alerting system (CRITIC alarm, such as a bell, voice intercom, internal telephone, or buzzer) installed between the appropriate operations area surveillance and warning (S&W) center and the CSF, and RCSF. Operations personnel use this system to alert the CSF, or RCSF of an impending CRITIC message. Use this alarm only for valid CRITIC and NSA-directed CRITIC tests only.

e. Check the system used by operations to alert the CSF, RCSF of an impending CRITIC message. Record such checks in the master station log. Checks should be made at the beginning of each shift.

f. Ensure that original transmissions are accurate to prevent follow-up transmission. Proofread the CRITIC immediately after transmission. Establish a service CRITIC mask that can be used to service CRITIC messages in the event the CRITIC must be serviced.

g. Ensure that operating instructions identify all alternate routes and methods which a CRITIC message may be transmitted as required by DOI-103 (including military affiliated radio station (MARS), automatic secure voice communications, secure terminals units, third generation (STU-III), operations communications (OPSCOMM, or defense CRITICOMM communications (DCC) orderwire.

h. Alternate routes to transmit a CRITIC or NSA-directed CRITIC test message are listed in order of precedence to facilitate timely message processing.

i. No CRITIC messages are rejected for transmission because of improper format. Brief any problems with the CRITIC to the originator after transmitting the CRITIC and list those problems in paragraph four of the CRITIC handling report.

j. Complete applicable blocks on the AIA Form 72, (FOUO) CRITIC Checklist, for each CRITIC, NSA directed CRITIC, and in-station CRITIC test message. Ensure that a completed critique is done, and that all required actions are taken. File the CRITIC, AIA Form 72, and any amplifying information together.

k. Ensure that an acknowledgment of receipt is sent to NEWSDEALER remote terminals from which CRITIC messages are received. A procedure wire "R W" is sent within 2 minutes of receipt of the CRITIC message.

5.2.14. (Added) NSA-Directed CRITIC Message **Handling.** NSA schedules CRITIC exercise messages. The exercise message is delivered to the CSF, and RCSF by means and procedures normally used for a valid CRITIC message. The CRITIC action officer is contacted to ensure that management personnel are available to monitor NSA-directed CIUTIC tests. NSA-directed CRITIC tests are processed as a valid CRITIC unless otherwise notified.

5.2.15. (Added) When required, CRITIC tests are transmitted by OPSCOMM circuits when directed by NSA.

5.2.16. (Added) S&W personnel are responsible for completing the handling and processing of OPSCOMM CRITIC messages. They notify communications operations personnel to stand by in the event OPSCOMM transmission should fail. If there is an abnormal condition during the release period (special mission or exercise, significant volume of high precedence traffic, or complete outage of OPSCOMM circuits), the operations officer reschedules or cancels the test.

5.2.17. (Added) CRITIC Handling Reports (RCS: NSA-972). Prepare and forward according to DOI-103. If a CRITIC is transmitted via means transparent to the communications function (OPSCONW, voice, etcetera), the operations officer provides the necessary information to the SC as outlined in USSID 301, paragraph 8.3.

a. All stations originating or relaying a CRITIC include HQ AIA/SCXI and intermediate headquarters as information addresses on all CRITIC correspondence.

b. Indicate in parenthesis, after the subject line of the report, whether the CRITIC was an NSA-directed test or a valid CRITIC, and the CRITIC number.

c. When a CRITIC test is transmitted from the S&W center, SC personnel assist the operations personnel in preparing and forwarding the handling report.

d. Any problems or abnormalities associated with the processing of a CRITIC (valid or NSA-directed) are included in paragraph four of the handling report.

5.2.18. (Added) In-Station CRITIC Test:

a. Communicators involved in CRITIC handling perform at least two in-station CRITIC tests a month. The shifts supervisor administer these tests. Alert all personnel by announcing in a loud voice" in-station CRITIC test!" Additionally, management personnel, the superintendent, the Noncommissioned Officer in Charge (NCOIC), or the M&R section are responsible for releasing and monitoring an in-station test for each shift at least once a month. Test procedures are designed to prevent on-line transmission. The following examples are to be used as message narrative for in-station testing. All CSFs, RCSFs, will perform CRITIC testing using a stand-alone computer (PC).

(1) THIS IS AN IN-STATION TEST OF CRITIC HANDLING AND PROCEDURES. DO NOT TRANSMIT THIS MESSAGE. IF INADVERTENTLY TRANSMITTED, RECEIVING STATIONS WILL DISREGARD. END OF TEST.

(2) TIUS CRITIC MESSAGE IS AN IN-STATION TEST. DO NOT ATTEMPT ON-LINE TRANSMISSION OF THIS MESSAGE. ANY RECEIVING STATION IS TO DISREGARD ITS RECEIPT. END OF TEST.

(3) TEST CRITIC MESSAGE FOR IN-STATION USE ONLY. PREPARE THE TEST AS REALISTICALLY AS POSSIBLE. MAKE NO ATTEMPTS TO TRANSMIT THIS MESSAGE. DISREGARD IF RECEIVED. END OF TEST.

(4) THIS IS A CRITIC IN-STATION TEST. PROCESS THE MESSAGE WITH AS MUCH REALISM AS POSSIBLE. ENSURE THAT THIS MESSAGE IS NOT TRANSMITTED. ANY RECEIVING STATION WILL DISREGARD. END OF TEST.

b. **NOTE:** DO NOT PERFORM IN-STATION CRITIC TESTING USING ANY COMPUTER SYSTEM CONNECTED TO AN ON-LINE SYSTEM (i.e., NEWSDEALER, AMHS, MPS, CSP, MCS, Local Area Network (LAN), etcetera).

5.3. (Added) Customer-Operated Remote (COR) Facilities. This section outlines the operational concept for COR facilities and applicable policies, procedures, and responsibilities. CORs are connected on-line to a host NEWSDEALER facility and operated by the customer to transmit and receive DSSCS and GENSER record message traffic.

a. Concept of Operations. COR facilities employ the minimum operating procedures required to provide secure, accurate, and expeditious message processing. This includes maintenance of records required to ensure message continuity and record of receipt (when required). If a 3CXY.X communicator is assigned to the unit, they are identified to act as a "communications liaison" to assist the customer when problems are experienced in message processing. Additionally, if a 3CXXX is assigned, they are responsible for the drafting of communication policies necessary to ensure the customer receives secure and reliable communications.

b. Publications. COR facilities maintain the host's NEWSDEALER Customer Education Guide.

c. Forms. Forms necessary to maintain message accountability and continuity are required. Non-AIA COR facilities use comparable forms as prescribed by their major command or service (Army, Navy).

d. Equipment. Equipment identified in the requesting units accreditation package and approved for use by the NEWSDEALER configuration control authority are used as the end terminal equipment. This equipment is normally a personal computer which meets TENWEST requirements.

e. Responsibilities.

(1) Processing Incoming and Outgoing Message Traffic. The COR facilities ensure the continuity of incoming and outgoing message traffic is maintained at all times. This requirement can be satisfied by using the AF Form 3534, Channel Number Sheet, or a general purpose form.

(2) General Personnel Responsibilities. There are certain general responsibilities common to all supervisory or operator personnel performing duties in the COR. The unit appoints a COR system administration in writing. The COR will:

(a) Develop station operating procedures for proper control of SPECAT, LIMDIS, Personal For, collateral Top Secret, and other special handling caveats.

(b) Provide the host NEWSDEALER with the name, telephone number (secure and unsecure) of the point of contact for the COR terminal.

(c) Provide the host NEWSDEALE, when applicable, the part time hours of operations and procedures for notification of high-precedence message traffic during other than normal duty hours.

(d) Develop an alternate route agreement for processing high-precedence traffic during extended periods of outage on their terminal.

(e) Assign IDs to all personnel authorized to log-on and process messages on the CORs terminal.

(f) Act as the focal point for system training, directing questions to their on-site communications consultant, the host, wing, group or HQ AIAISCXI as appropriate.

(g) Maintain the COR magnetic media inventory.

(h) Load the current version of the ABOVEBOARD software on the COR's terminals.

f. Assistance Request. Whenever COR personnel require assistance with message processing, they contact the on-site communications consultant, if one is available. If not,, consult with the NEWSDEALER host. This may be done via message address to NEWSDEALER HOST//ASSISTANCE REQUEST//, using DDI "DSH"," or another agreed upon message address, or it may be accomplished via secure telephone (STU-III).

g. PLA Updates. CORs submit all request for actions, changes, or deletions to the host NEWSDEALER plain language address tables using PLA: ROUTING UPDATE, or as directed in the Host Customer Brochure.

JANES M. ENGER, Colonel, USAF
Air Intelligence Agency, Director of C4I

Attachment
5. **(Added)** General Message Titles

Glossary of References, Abbreviations, and Acronyms

Section A-References: See paragraph 3.5 of this supplement.

Section B-Abbreviations and Acronyms

Abbreviations and Acronyms

ABOVEBOARD	NSA developed software for message processing
ACP	Allied Communications Publication
AFIWC	Air Force Information Warfare Center
AIG	Address Indicator Group
ALREMOTE	All Remote Customers Connected to AIA NEWSDEALERS
ALT HQ	Alternate Headquarters
ASCII	American Standard Code for Information
ALT HQ	Alternate Headquarters
ASCII	American Standard Code for Information
AUTODIN	Automatic Digital Network
BUSTER	Program on TOOLBOX to detect unauthorized information
C-CS	Communications-Computer Systems
CIM	Communications Improvement Memorandum
COI	CRITICOMM Operating Instructions
COMOPS	Communications Operating Performance Summary
COMSEC	Communications Security
COR	Customer Operated Remote
CRITIC	Contains information of vital importance - Handled above all other messages
CRITICOMM	Critical Intelligence Communications
CSF	CRITICOMM Support Facility
CSO	C4I System Officer
CSP	Communications Support Processor
CSRD	Communications-Computer Systems Requirement Document
DAG	Defense Special Security Address Group
DDI	Delivery Distribution Indicator
DEFCON	Defense Condition
DIACAB	DIA Compartmented Address Book
DISA	Defense Information Systems Agency
DOI	Defense Special Security Communications System Operating Instructions
DPC	Data Processing Center
DSSCS	Defense Special Security Communications Systems

ERROR	Errored message sent back to customer from NEWSDEALER
ERS	Emergency Relocation Station
FAS	Functional Address Symbol
FEEDBACK	Automatic comeback copy of messages from NEWSDEALER
FOA	Field Operating Agency
GENSER	General Service
HQ AIA	Headquarters Air Intelligence Agency
JANAP	Joint Army-Navy-Air Force Publication
JC2WC	Joint Command Control Warfare Center
LIMDIS	Limited Distribution
M&R	Methods and Results
MINIMIZE	Limit Volume of non-essential message traffic
MML	Message Management Letter
MS	FAS For C4 operations at supported HQ AIA Field Units
NEWSDEALER	NSA Developed Communications Message Processing System
OPSCOMM	Operations communications
PLA	Plain Language Address
PLA SEARCH	Software program to check for PLAs
RW	Receipt acknowledgment for a CRITIC message
RADAY	Radio Day
RCSF	Remote CRITICOMM Support Facility
S&W	Surveillance and Warning
SC	FAS For C4 operations at HQ AIA Field Units
SO	FAS For Security at supported HQ AIA Field Units
SCI	Special Compartmented Information
SPECAT	Special Category
SSO	Special Security Officer
TOOLBOX	Software used to detect viruses
USAFINTEL	United States Air Force Intelligence
USSID	United States Signals Intelligence Directive
ZDF-1	Acknowledgment of Delivery From Addressee
ZDF-2	Acknowledgment of Delivery From Addressee Comm Center
ZDS	Corrected Copy (GENSER)
ZEN	Delivered by other means
ZZS	Corrected Copy (DSSCS)

Section C-Definitions

CRITICOMM Support Facility (CSF): CSFs are AIA NEWSDEALER communications operations that process DSSCS and GENSER message traffic and are tied into the Defense Communications System (DCS). NEWSDEALER systems are tied directly into the automatic digital network (AUTODN, or the National Security Agency global communications systems (GCS) network.

RCSF: RCSFs are NEWSDEALER remote operations that are operated by communications-computer operations personnel. They are not required to fulfill all the requirements of a CSF (NEWSDEALER host). It must be noted that certain AIA RCSFs connected to Army, Navy or NSA NEWSDEALER systems are required to comply with (in addition to certain provisions of AIA Supplement 1 to AFI 33-113) the host policies and procedures for operating their remote terminal. The RCSF is responsible for ensuring proper message accountability and control of all originated and terminated message traffic. Accountability of message traffic is satisfied by using AF Form 3534, Channel Number Sheet.

COR: A COR is defined as any remote communications terminal that is operated solely by the customer. It includes only those communications-computer systems functions which are necessary to send and, or receive the COR's information. They rely on the host automated message processing exchange (ANTE) for network control. It must be noted that certain AIA RCSFs connected to Army, Navy or NSA NEWSDEALER systems are required to comply with (in addition to certain provisions of AIA Supplement 1 to AFI 33-113) the host policies and procedures for operating their remote terminal. The RCSF is responsible for ensuring proper message accountability and control of all originated and terminated message traffic. Accountability of message traffic is satisfied by using AF Form 3534, **Channel Number Sheet.**

Communications Support Processor (CSP): CSP is a versatile, secure message processing system that provides trusted handling of GENSER and DSSCS traffic. CSP is used in multiple roles, including fixed based, mobile, and tactical communications.

Attachment 5 **(Added)**

Introduction. The following general message titles include HQ USAF, AIA and NON-USAF (applicable to USAF organizations).

A5. 1. HQ USAF Titles

A5. 1. 1. ALMAJCOM-FOA. Message originator. HQ USAF, addressed to all major commands and separate Field Operating Agencies (FOA). FOA's will include direct reporting units.

A5.1.2. ALZICOM-FOA. Message originator: HQ USAF, addressed to Continental United States (CONUS) MAJCOMs and FOAS. FOAs will include direct reporting units.

A5.1.3. ALMAJCOM. Message originator. HQ USAF, addressed to all MAJCOMS.

A5.1.4. ALZICOM. Message originator: HQ USAF, addressed to CONUS MAJCOMS.

A5.1.5. ALPERSCOM. Message originator and purpose: USAF Military Personnel Center, Randolph Air Force Base, Texas, addressed to all MAJCOMs and FOAs concerning general subject of military personnel.

A5.1.6. ALDODACT. Message originator and purpose: For the exclusive use of the Secretary of Defense to disseminate unclassified information to all installations and activities throughout the Department of Defense.

A5.2. AIA Titles:

A5.2.1. ALAIACOMSTA. Message originator and purpose: A general message assigned to AIA used to issue guidance and instructions to all AIA and AIA supported organizations which operates a Data Processing Center (DPC), CRITICOMM Support Facility (CSF), and Customer Operator Remote (COR Facility which have agency application.

A5.2.2. (All Connected AIA NEWSDEALER Remotes). Message originator and purpose. A general message assigned to AIA NEWSDEALER facilities for use by the system administrator to issue MINIMIZE information and other guidance or instructions to all in-house and distant NEWSDEALER remote customers.

A5.3. NON-HQ USAF Titles: (Applicable to USAF Organizations)

A5.3. 1. ALNMACT. Message originator and purpose: Joint Chief of Staff (JCS), uses to impose MINIMIZE or to issue other instructions or information having worldwide application.

A5.3.2. ALSVCAT. Message originator and purpose: JCS uses to impose MINIMIZE or to issue other instructions on a classified basis having worldwide application.

A5.3.3. JAFPUB. Message originator and purpose: JCS uses to issue corrections to JANAs and ACPs including supplements that require wide distribution.

A5.3.4. EUCOMACT. Message originator and purpose: A general message title assigned to United States Commander in Chief, Europe, (USCINCEUR) to impose MINIMIZE or other instructions or information which have USCINCEUR command application.

A5.3.5. JANAPAFPAC. Message originator and purpose: A general message title assigned to CINCPAC and addressed to US MAJCOMs within the Pacific Command on matters of joint interest. Redistribution is accomplished at the discretion of the receiving US MAJCOM.

A5.3.6. LANTCOMACT. Message originator and purpose: A general message assigned to Commander in Chief, Atlantic, to impose MINIMIZE or other instructions or information which have Atlantic Command application.

A5.3.7. PACOMACT. Message originator and purpose: A general message title assigned to CINCPAC to impose MINIMIZE or other instructions or information which have Pacific Command application.

A5.3.8. USSOCOMACT. Message originator and purpose: A general message title assigned to US Commander in Chief, Southern Command. to impose MINIMIZE or other instructions or information which use military communications.